99TH CONGRESS
2d Session

HOUSE OF REPRESENTATIVES

REPT. 99-753
Part 2

COMPUTER SECURITY ACT OF 1986

NEWARK PUBLIC LIBRARY

AUGUST 6, 1986.—Committed to the Committee of the Whole House on the State of the Union and ordered to be printed

AUG 25 1986

Mr. BROOKS, from the Committee on Government Operations, submitted the following

U.S. GOVT. PUBS.
DEPOSITORY 376

REPORT

[To accompany H.R. 2889 which on June 27, 1985, was referred jointly to the Committee on Science and Technology and the Committee on Government Operations]

[Including cost estimate of the Congressional Budget Office]

The Committee on Government Operations, to whom was referred the bill (H.R. 2889) to amend the act establishing the National Bureau of Standards to provide for a computer security research program within such Bureau, and to provide for the training of Federal employees who are involved in the management, operation, and use of automated information processing systems, having considered the same, report favorably thereon with an amendment and recommend that the bill as amended do pass.

The amendment is as follows:

Strike out all after the enacting clause and insert in lieu thereof the following:

SECTION 1. SHORT TITLE.

This Act may cited as the "Computer Security Act of 1986".

SEC. 2. FINDINGS.

The Congress finds that—

(1) in recent years the Federal Government has become highly dependent on automated information processing systems for carrying out many of its missions;

(2) the Government operates about 20,000 medium- and large-scale mainframe computers and by the end of this decade it will also have approximately half a million micro- and mini-computers;

(3) the information stored in Government computers and transmitted over the various communications networks that connect them represent valued property that is vulnerable to unauthorized access and disclosure, fraudulent manipulation, and disruption;

(4) studies of computer-related fraud and abuse in Government agencies indicate a costly and widespread problem of significant proportions;

62-648 O

Y1.1/8:

(5) Government efforts to address the problems of computer security have focused on developing hardware and software systems to protect sensitive information, ensuring that new computer systems are designed to include security provisions, and requiring agencies to implement security procedures; and

(6) these efforts must be supplemented if the problems are to be solved, since the weak link in protecting the information stored, processed, and transmitted by Government computers remains the people who manage, use and operate them.

SEC. 3. ESTABLISHMENT OF COMPUTER SECURITY MANAGEMENT, RESEARCH, AND TRAINING PROGRAM.

The Act of March 3, 1901 (15 U.S.C. 271–278h), is amended by redesignating section 18 as section 20, and by inserting after section 17 the following new sections:

"SEC. 18. (a) The National Bureau of Standards shall have the sole authority and responsibility for establishing and conducting a computer security management, research, and training program pertaining to computer and telecommunications systems that are subject to the provisions of section 111 of the Federal Property and Administrative Services Act of 1949 (40 U.S.C. 759) or chapter 35 of title 44, United States Code. The primary emphasis of such program shall be the prevention of computer-related fraud and abuse. For such purpose, the Bureau shall prepare and submit to the Secretary of Commerce, for promulgation under such section 111, government-wide standards and guidelines.

"(b) In carrying out the program described in subsection (a), the Bureau shall—

"(1) perform research and conduct studies to determine the nature and extent of the vulnerabilities of computer and telecommunications systems in Federal agencies and their contractors;

"(2) devise management, administrative, technical, and physical procedures and practices designed to protect the information stored, processed, and transmitted by Government computer and telecommunications systems;

"(3) develop standards and guidelines for the security of such computer and telecommunications systems and offer assistance for use by Federal agencies in training their employees, and the employees of their contractors and of other organizations whose computer or telecommunications systems interface with Government computer systems, in computer and telecommunications security awareness and accepted security practices;

"(4) make recommendations to the General Services Administration on computer and telecommunications security policy and on revisions of regulations proposed pursuant to section 111(f)(3) of the Federal Property and Administrative Services Act of 1949;

"(5) develop and coordinate, as appropriate, with the General Services Administration, the Office of Personnel Management, and the National Security Agency, joint computer and telecommunications security standards, research, and training programs;

"(6) validate the effectiveness of computer and telecommunications security standards through research, inspection, and reporting activities;

"(7) act as liaison between the Federal Government and the private sector with respect to computer and telecommunications security issues involving sensitive but unclassified information and assist the private sector in using and applying the results of the programs and activities under this section; and

"(8) establish an advisory council composed of representatives of other Federal agencies.

"SEC. 19. (a) There is hereby established a Computer and Telecommunications Privacy and Security Advisory Board within the National Bureau of Standards. The Secretary of Commerce shall appoint the chairman of the Board. The Board shall be composed of twelve additional members appointed by the Secretary of Commerce as follows:

"(1) four members from outside the Federal Government who are eminent in the computer or telecommunications industry, at least one of whom is representative of small or medium sized companies in such industry;

"(2) four members from outside the Federal Government who are eminent in the fields of computer or telecommunications technology, or related disciplines, but who are not employed by or representative of a producer of computer or telecommunications equipment; and

"(3) four members from the Federal Government who have computer or telecommunications systems management experience, including experience in computer security or telecommunications security, at least one of whom shall be from the National Security Agency.

"(b) The duties of the Board shall be—

"(1) to identify emerging managerial, technical, administrative, and physical safeguard issues relative to computer and telecommunications systems security; and

"(2) to advise the Bureau of Standards and the Secretary of Commerce on security and privacy issues pertaining to computer and telecommunications systems of the Federal Government.

"(c) The term of office of each member of the Board shall be four years, except that—

"(1) of the initial members, three shall be appointed for terms of one year, three shall be appointed for terms of two years, three shall be appointed for terms of three years, and three shall be appointed for terms of four years; and

"(2) any member appointed to fill a vacancy in the Board shall serve for the remainder of the term for which his predecessor was appointed.

"(d) The Board shall not act in the absence of a quorum, which shall consist of seven members. Members of the Board, other than full-time employees of the Federal Government, may be compensated at a rate not to exceed the maximum rate of pay for grade GS–18, as provided in subchapter III of chapter 53, title 5, United States Code, when engaged in the actual performance of duties vested in the Board.

"(e) Members of the Board, other than full-time employees of the Federal Government, while attending meetings of such committees or while otherwise performing duties at the request of the Board Chairman while away from their homes or a regular place of business, may be allowed travel expenses in accordance with subchapter I of chapter 57 of title 5, United States Code.

"(f) To provide the staff services necessary to assist the Board in carrying out its functions, the Board may utilize personnel from the National Bureau of Standards or any other agency of the Federal Government with the consent of the head of the agency.".

SEC. 4. AMENDMENT TO BROOKS ACT.

Section 111(f) of the Federal Property and Administrative Services Act of 1949 (40 U.S.C. 759(f)) is amended to read as follows:

"(f)(1) The Secretary of Commerce shall—

"(A) provide agencies, and the Administrator in the exercise of functions delegated in this section, with scientific and technological advisory services relating to automatic data processing and related systems, including telecommunications systems;

"(B) establish uniform Federal automatic data processing and related telecommunications standards and guidelines; and

"(C) on the basis of standards and guidelines developed by the Nationl Bureau of Standards pursuant to section 18(b)(3) of the Act of March 3, 1901 (15 U.S.C. 271 et seq.), establish standards and guidelines for the security of computer and telecommunications systems that are subject to this section.

"(2) The standards established by the Secretary of Commerce under paragraphs (1)(B) and (1)(C) shall be compulsory and binding on each Federal agency unless waived by the Secretary of Commerce in writing upon a determination that compliance would adversely affect the accomplishment of the agency's mission or cause a major adverse financial impact on the agency which is not offset by government-wide savings. Notice of each such waiver shall be promptly transmitted to the Committee on Government Operations of the House of Representatives and the Committee on Governmental Affairs of the Senate.

"(3) The Administrator shall ensure that such standards and guidelines are implemented within an integrated information resources management system (as required by chapter 35 of title 44, United States Code) by—

"(A) developing and implementing policies on the security of automatic data processing and related telecommunications systems; and

"(B) revising the Federal information resources management regulations (41 CFR ch. 201) consistent with such standards, guidelines, and policies.

"(4) In carrying out functions under paragraph (1) of this subsection, the Secretary of Commerce and the Director of the National Bureau of Standards are authorized—

"(A) to accept, hold, administer, and use gifts and bequests of property, both real and personal, for the purpose of aiding or facilitating such functions; and

"(B) to accept reimbursement for the performance of such functions for the benefit of another Federal agency or for the benefit of any other person or organization, at rates approximating the costs thereof.

"(5) The Secretary is authorized to undertake the necessary research in the sciences and technologies of automatic data processing computer and related systems,

including telecommunications systems, as may be required under the provisions of this subsection.".

SEC. 5. TRAINING BY FEDERAL AGENCIES IN COMPUTER AND TELECOMMUNICATIONS SECURITY.

(a) IN GENERAL.—Each Federal agency (as that term is defined in section 3(b) of the Federal Property and Administrative Services Act of 1949) shall provide mandatory periodic training in computer and telecommunications security. Such training shall be provided under the guidelines developed pursuant to section 18(b)(3) of the Act of March 3, 1901 (as added by section 3 of this Act), and in accordance with the regulations issued under subsection (c) of this section, for all of the agency's employees who are involved with the management, use, or operation of computer or other automated information systems, including related telecommunications systems, and for all of the employees and other personnel of its contractors who are involved with the management, use, or operation of computers which interface with Government systems.

(b) TRAINING OBJECTIVES.—Training under this section shall be started within 60 days after the issuance of the regulations described in subsection (c). Such training shall be designed—

(1) to enhance employees' awareness of the threats to and vulnerability of computer and telecommunications systems; and

(2) to encourage the use of improved computer security practices at Government facilities.

(c) REGULATIONS.—Within six months after the date of the enactment of this Act, the Director of the Office of Personnel Management shall issue regulations prescribing in detail the procedures and scope of the training to be provided by Federal agencies under subsection (a) and the manner in which such training is to be carried out.

SEC. 6. ADDITIONAL FEDERAL AGENCY RESPONSIBILITIES FOR COMPUTER AND TELECOMMUNICATIONS SECURITY.

(a) IDENTIFICATION OF SENSITIVE SYSTEMS.—Within 6 months after the date of enactment of this Act, each Federal agency (as that term is defined in section 3(b) of the Federal Property and Administrative Services Act of 1949) shall identify each computer and related telecommunications system of that agency within which is or will be stored or through which is or will be transmitted sensitive (but unclassified) information the loss or misuse of which could adversely affect the national interest or the conduct of Federal programs.

(b) SECURITY PLAN.—Within one year after the date of enactment of this Act, each such Federal agency shall, consistent with the standards, guidelins, policies, and regulations prescribed pursuant to section 111(f) of the Federal Property and Administrative Services Act of 1949, establish a plan for the security of the computer and related telecommunications systems and systems in development identified pursuant to subsection (a). Copies of such plan shall be transmitted to the National Bureau of Standards and the National Security Agency for advice and comment. Such plan shall be subject to disapproval by the Administrator of General Services.

SEC. 7. AUTHORIZATION OF APPROPRIATIONS.

There are hereby authorized to be appropriated to the National Bureau of Standards for the fiscal years 1987, 1988, and 1989 to carry out the computer security management, research, and training program established by this Act, such sums as may be necessary. There are also authorized to be appropriated to each Federal agency such sums as may be necessary for fiscal years 1987, 1988, and 1989 to carry out the computer and telecommunications security training program established by section 5 of this Act and the identification and planning requirement of section 6.

SUMMARY AND PURPOSE

H.R. 2889 establishes a new research program within the National Bureau of Standards (NBS) to assess the vulnerability of government computers and communications. It also provides for the development of technical and management techniques to defend against unlawful access to sensitive government information. Federal agencies would be required to provide mandatory training for their employees in computer and communications security.

H.R. 2889 is the result of growing concern within the Congress that the government's computer and communications systems are

READEX FICHE best copy available

not being adequately protected from unauthorized access, or misuse. This Committee has over the years conducted extensive investigations of computer and communications facilities of several major Federal agencies. In almost every case, security was lax or virtually non-existent. Notwithstanding, computer and communications security has remained a low priority for most Federal agencies and a relatively small amount of funds has been devoted to this area.

Apparently to stop the foreign exploitation of our nation's computer based information systems, the President issued in September of 1984 National Security Decision Directive 145: National Policy on Telecommunications and Automated Information Systems Security. Under this directive, the Department of Defense (DOD) was given broad new powers to issue policies and standards for the safeguarding of not only classified information, but also other information in the civilian agencies and private sector which DOD believed to be "sensitive." The National Security Agency (NSA), whose primary mission is one of foreign intelligence, was given the responsibility of managing this program on a day-to-day basis.

The issuance of NSDD–145 raised considerable concern within the public and the Congress. First, it expanded DOD's authorities beyond its typical role of protecting classified information to deciding what unclassified information should be protected. Second, it gave NSA the authority to use its considerable foreign intelligence expertise within this country. This is particularly troubling since NSA was not created by the Congress, but by a secret presidential directive and it has, on occasion, improperly targeted American citizens for surveillance. The potential for further abuse by that agency under NSDD–145 is considerable. Third, the Directive is in conflict with current law, which assigns authorities and responsibilities for the development of computer and communications standards to agencies other than DOD. Under both the Brooks Act (P.L. 89–306) and the Paperwork Reduction Act (P.L. 96–511), the Office of Management and Budget (OMB), the General Services Administration (GSA), and the Commerce Department have government-wide management and policy responsibilities for computers, telecommunications and information management, including authority for the issuance of policies and standards for computer security.

H.R. 2889 contains provisions to resolve these problems inherent in NSDD–145 while at the same time providing a statutory mandate for a strong security program that includes both NBS and NSA. The bill assigns to NBS the responsibilities for the establishment of computer and communications security standards on a government-wide basis in accordance with the Brooks Act and the Paperwork Act. In recognition of NSA's expertise in this area, that agency is given for the first time a statutory role in assisting NBS in its government-wide standard-setting duties. NSA is also allowed to continue its computer security work in those Defense systems which are currently exempted from the Brooks Act and the Paperwork Act.

H.R. 2889 requires each agency to identify its own sensitive information (not DOD) which may need protection and, in addition, de-

velop a computer security plan outlining its proposed efforts to protect this information. Copies of the plan are to be sent to both NBS and NSA for review and comment. The Adminstrator of GSA has the authority to disapprove an agency's plan if it is found to be deficient.

H.R. 2889 also establishes an advisory board consisting of outside experts, government officials and those in private industry to advise NBS in its work. NSA is required to serve as one of these advisors.

H.R. 2889 authorizes such funding as is necessary for Fiscal Years 1987, 1988, and 1989 to both NBS and Federal agencies in their efforts to develop standards, increase security awareness and to provide adequate protection for their computer and communications systems.

Committee Action and Vote

H.R. 2889 was introduced by Congressman Dan Glickman on June 27, 1985, and subsequently referred jointly to the Committee on Science and Technology and Government Operations. The Committee on Government Operations ordered the bill reported as amended on October 29, 1985, by a unanimous voice vote with a quorum present.

Hearings

Hearings on H.R. 2889 were held by the Subcommittee on Legislation and National Security on September 18, 1985. Testimony was received from Congressman Dan Glickman (D-Kans.) and representatives of the Department of Commerce, the Institute for Computer Sciences and Technology of the National Bureau of Standards, the Department of Defense, the National Security Agency, the General Accounting Office, the American Civil Liberties Union, the Institute of Electrical and Electronics Engineers, Inc., the Office of Technology Assessment, and the Computer and Communications Industry Association.

Explanation of Amendment

Inasmuch as all after the enacting clause of H.R. 2889 was stricken and all language incorporated into one amendment, this report constitutes an explanation of the amendment.

Discussion

BACKGROUND

Over the last thirty years, the government has greatly expanded its use of computer and communications technology. Current estimates from the Office of Technology Assessment (OTA) indicate that over $60 billion is spent annually by Federal agencies to acquire, develop and use this technology in automating its operations.[1] Although the information technology revolution has great-

[1] Federal Government Information Technology: Management Security, and Congressional Oversight, Office of Technology Assessment, February 1986. Note: OTA estimates the Federal Government has about 27,000 mainframe computers, over 100,000 microcomputers, and over 170,000 mainframe computer terminals.

ly increased the efficiency of government programs at reduced costs, it has also made virtually every agency dependent on its use. Moreover, the potential for abuse of this technology is enormous. For example, information is maintained by the Internal Revenue Service and the Social Security Administration on virtually every citizen of the United States which, if altered, manipulated, or destroyed, could affect the privacy of these individuals. Further, the Federal Reserve System transmits billions of dollars every day over its communications lines which, if tampered with, could affect the viability of our nation's economy.

During the 1960's and early 1970's, Federal agencies could with a reasonable degree of assurance protect their computer system and data files because most of the processing was being done at central sites. However, with the advent of mini and micro technology, coupled with on-line access, the aforementioned protection ceased to exist. Today, any knowledgeable computer person can tap into almost any computer system thousands of miles away. There have been many stories in the press about hackers who have managed with relative ease to enter a computer system containing sensitive information and manipulate it for their own purposes. School systems, banks, and even the Defense Department have not been able to stop these unwarranted intrusions. On a more malicious level, credit card information and even tax records have been altered or destroyed and the use of computers for theft and fraud has been on the rise over the last five years.

Unfortunately, efforts by the Federal Government to establish a computer security program have not kept pace with the rapidly changing technology. Most agencies have placed such a low priority in protecting its computer systems that even the most basic computer security measures, i.e. physical and administrative, do not exist. Not surprisingly, little effort has been made to use the technology itself to secure the computer systems from outside penetration. This lack of computer security is a serious problem since such systems are the core of every modern organization. Destruction of these systems would undoubtedly bring the operations of these organizations to an abrupt halt and the effect of this on our citizens would be catastrophic.

H.R. 2889 is designed to establish a credible computer security program for the Federal Government. It establishes a new research program within the National Bureau of Standards (NBS) to assess the vulnerability of government computers and communications. It provides for the development of technical and management techniques to defend against unlawful access to sensitive government information and for mandatory training for Federal employees. It also creates a computer security board composed of experts from the government and the private sector and requires agencies to identify sensitive information and develop plans to protect that information. Finally, it clearly delineates the roles of NBS and NSA in regard to these activities in the computer security program.

FEDERAL COMPUTER STANDARDS PROGRAM

With the passage of the Brooks Act (P.L. 89-306) in 1965, the Department of Commerce was given the responsibility for the development and issuance of Federal computer standards. Pursuant to its enactment, the Institute of Computer Sciences and Technology (ICST) was established within the National Bureau of Standards to fulfill the responsibilities given to the Department of Commerce by the Brooks Act. The Paperwork Reduction Act of 1980 (P.L. 96-511) reinforced the role of ICST and the Commerce Department in the development of computer standards. In recognition of the importance of information technology and the vital role that Federal standards place in using that technology, this law further called on the OMB to revitalize the standards program.

In fulfilling its statutory mandate, the Institute conducts research and provides technical support to the development of national and international standards for computer software and hardware, including computer networks. The Institute's work has benefitted Federal, State and local governments as well as the private sector, particularly our nation's computer industry. It has issued over 100 standards and technical guidance documents and provided valuable technical assistance and leadership in both the national and international standards areas.

In regard to computer security, the Institute recognized as far back as 1972 that it would be a major concern for users of the technology. At that time, it initiated its Computer Security and Risk Management program. This program encompasses research and development of security standards, transfer of technology to potential implementors and vendors, and assistance to users of security technology. Numerous standards, guidelines and technical reports have been issued in the areas of physical security, technical security and computer security management. The Institute has also established comprehensive programs in computer reliability and integrity, i.e. detecting unauthorized entry or change of information as well as confidentiality to prevent unauthorized disclosure of information.

Unfortunately, despite the considerable achievements by the Institute, efforts have been made by the Administration over the last five years to cut drastically the funding of this important program. These cuts are being made without regard to the significant benefits that have been achieved by the program. The issuance of 54 Federal Information Processing Standards (FIPS) by the Institute is saving the government about $132 million annually—thirteen times the annual budget of the Institute.[2] Fortunately, this Committee and the Science and Technology Committee have worked to successfully restore the funding to the Institute.

NSDD-145

Apparently to counter the growing threat of foreign exploitation of computer-based information systems within both the government and the private sector, the President issued National Security

[2] These figures were provided by Joe Wright, then Deputy Secretary of Commerce, on October 21, 1981, in testimony before the Subcommittee on Legislation and National Security, Committee on Government Operations.

Decision Directive (NSDD 145). This Directive seeks to vest in the Department of Defense (DOD) the authority to establish regulations and standards that would govern the access to and the processing of all computerized information which DOD deems to be critical to the national security of the United States. This would include not only classified information, but any other information within the civilian agencies that the Department considers to be in the interest of national security. Under the Directive, virtually any information system located in the civilian agencies or the private sector would fall under its domain.

Sensitive information

One of the benefits of a full and open society is the rich exchange of ideas and knowledge unfettered by governmental intervention and redtape. The successes of our scientific, technical, and medical communities have been based upon the free exchange of data and information. Since it is a natural tendency of DOD to classify everything, it would be impossible for the Department to strike an objective balance between the need to safeguard information and the need to maintain the free exchange of information. There are other practical problems as well. First, DOD does not have the resources to classify and control all of the information that would be encompassed by this directive. Second, the cost of applying DOD-type security measures to civilian agency and private sector information systems would be overwhelming. Furthermore, DOD has its hands full trying to even modestly protect its own classified information and it would be foolhardy to expand its jurisdiction to protect the unclassified information contained in the civilian agencies and the private sector.

During the hearings, Assistant Secretary Donald Latham asserted that NSDD was being misread and that the directive was being misconstrued. He characterized NSDD-145 as a cooperative effort between Federal agencies and the private sector to improve the necessary computer and communications security whereby NSA and DOD would provide advice and assistance. According to Mr. Latham, NSDD-145 is "a much more benign document than others appear to think it is. . . ." [3] In fact, Mr. Latham went to great lengths during the hearings to allay the concerns of this Committee and many others that NSDD-145 is not intended to give NSA/DOD a free hand to control information throughout the government and the private sector. For example, Mr. Latham testified that:

> The purview of NSDD-145 is only for the former category [sensitive national security-related information and *not sensitive non-national security related information*]. (Emphasis added.)
>
> * * * * *
>
> Let me reiterate that NSDD-145 does *not cover unclassified but sensitive non-national security-related information* and, therefore, it in no way restricts, controls, or manages

[3] Hearing record, p. 62.

> the activities of other Federal departments or agencies who have responsibilities in non-national security-related areas. (Emphasis added.)
>
> • • • • •
>
> Again, NSDD–145 addresses only unclassified but sensitive national security related and *does not cover unclassified but sensitive non-national security-related information.*[4] (Emphasis added.)

Notwithstanding, in April 1986, NSA, who reports to Mr. Latham regarding computer security matters, announced that it was merging its Communications Security (COMSEC) and its Computer Security (COMPUSEC) organizations into an integrated organization called Information Security. In its announcement, the following was stated:

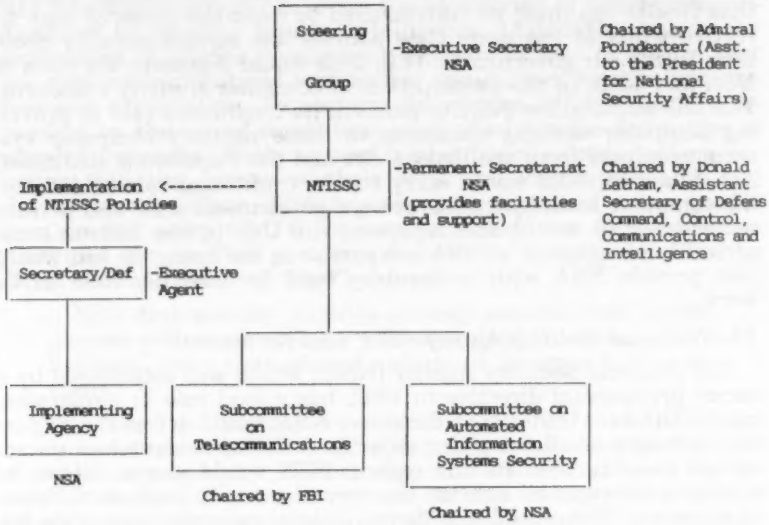
> The responsibilities of the new organization [within NSA] are being broadened under the auspices of National Security Decision Directive 145 *to include all computer security and communication security for the Federal Government and private industry,* including the protection of classified information; unclassified national security sensitive information; and *non-national security sensitive information.* (Emphasis added.)

This apparent broadening of responsibilities to include all information in the government and the private sector, including non-national security sensitive information was approved on December 20, 1985, by the NSDD–145 Steering Group—barely three months after Mr. Latham testified before the Committee.[5] No effort has been made by DOD to notify the Committee of the apparent change in position where important new powers were granted to DOD and NSA as a result of this December 20, 1985, decision. Under its current definition of "sensitive information," DOD and NSA have moved quickly to position themselves to directly influence the creation and dissemination of information within the civilian agencies and for that matter the country as a whole.

---

[4] Hearing record, p. 54.

[5] Mr. Latham's position under NSDD–145 is illustrated in the chart on page 11.


Steering Group
-Executive Secretary NSA
Chaired by Admiral Poindexter (Asst. to the President for National Security Affairs)
Implementation of NTISSC Policies
NTISSC
-Permanent Secretariat NSA (provides facilities and support)
Chaired by Donald Latham, Assistant Secretary of Defens Command, Control, Communications and Intelligence
Secretary/Def
-Executive Agent
Implementing Agency
NSA
Subcommittee on Telecommunications
Chaired by FBI
Subcommittee on Automated Information Systems Security
Chaired by NSA

Steering Group Membership

Secretary of State
Secretary of Treasury
Secretary of Defense
Attorney General
Director of OMB
Director of CIA

NTISSC Membership

Representatives of Steering Group
PLUS
Secretary of Commerce
Secretary of Transportation
Secretary of Energy
Chairman, JCS
Administrator, GSA
Director, FBI
Director, FEMA
Chief of Staff, USA
Chief of Naval Operations
Chief of Staff, USAF
Commandant, USMC
Director, DIA
Director, NSA
Manager, National Communications System

Note: Both the membership of the Steering Group and NTISSC is heavily weighted in favor of the Defense Department and the Intelligence agencies.

Given the concerns that Chairman Brooks and many others have expressed about the unwarranted intrusion by the military into the civilian agencies and the private sector, the Committee believes that NSDD–145 must be restructured to limit the scope of that directive while at the same time address the serious security problems facing our government. H.R. 2889 would delineate the roles of NSA and NBS, in the development of computer security standards. The bill would allow NSA to perform its traditional role of providing computer security measures to those military computer systems exempted from the Brooks Act and the Paperwork Reduction Act. Likewise, NBS would carry out its traditional role of developing computer security measures on a government-wide and private sector basis. It would also represent the U.S. in the international arena. In recognition of NSA's expertise in the area, the bill would also provide NSA with a statutory base for advising NBS in its work.

The National Security Agency—The need for secrecy

The National Security Agency (NSA), which was established by a secret presidential directive in 1952, has a lead role in implementing NSDD–145. Under that directive, NSA would act as the day-to-day manager of all computer security activities undertaken pursuant to the directive. In this regard, NSA would assess threats to sensitive systems and analyze the overall security posture of Federal agencies. NSA would also direct Federal agencies to provide the appropriate technology for the protection of automated information.

The appropriateness of having NSA, a super secret agency, appointed as the computer security "czar" under NSDD–145 raises serious questions. First, the role assigned to NSA under NSDD–145 would require the diversion of a substantial amount of resources from its national security mission to overseeing the protection of unclassified information in the civilian agencies and the private sector. Second, NSA's (and DOD's) natural tendency to restrict and even deny access to information that it deems important would disqualify that agency from being put in charge of the protection of non-national security information in the view of many officials in the civilian agencies and the private sector. Even in situations where NSA developed and proposed reasonable safeguards, implementation may be delayed or avoided altogether because of the inherent suspicions these officials may have about the motives of NSA. Finally, concern has been raised that giving NSA more authority to involve itself in the affairs of the civilian agencies and the private sector may tempt that agency to conduct domestic surveillance activities in violation of its charter.

The National Security Agency, since its establishment in 1952 by President Truman, has historically remained out of public view.[6] In fact, until 1962, NSA's existence was not even acknowledged in the U.S. Government Manual. No director of NSA ever appeared before a Congressional committee in public session until 23 years after its creation—1975. The first press interview was not given

[6] NSA was created by a top secret memorandum from President Truman to the Secretaries of State and Defense on October 24, 1952.

until 1978.[7] The reason for this secrecy is its unique mission which is two-fold—signal intelligence (SIGINT) and communications security (COMSEC). SIGINT involves the monitoring of foreign communications to produce foreign intelligence. COMSEC involves the monitoring of official government communications to ensure that our own communications systems are secure from foreign interception and exploitation. To perform its mission, NSA is heavily dependent on the use of computers, particularly in the decryption of encoded messages. Their success is also heavily dependent on ensuring that the results of their work are maintained with the utmost secrecy. Thus, NSA has always maintained a low profile even to the point that their very existence was kept from the American people. This penchant for secrecy is aptly described by David Kahn in his book, *The Codebreaker:* [8]

> NSA dins security security security security into its employees with remorseless persistence until it becomes more habitual, more than second nature—it becomes virtual instinct.

NSA's need for secrecy sometimes results in a rather heavy handed approach when it deals with public issues such as the issue of public cryptography. Historically, this science has been the exclusive domain of government and in this country it is one of NSA's primary missions. However, with the advent of modern computers and communications, there has been in recent years considerable interest in cryptography, particularly by the business community which is interested in keeping its proprietary information from competitors. As a result of the emerging need to protect information, the academic community has done research work in the field. NSA has made numerous attempts to either stop such work or to make sure it has control over the work by funding it, pre-publication reviews or other methods.[9]

The following contemporary account of one such incident is excerpted from the Congressional testimony of Frank A. Cassell, former Assistant Chancellor, UW-Milwaukee: [10]

> Professor Davida is a national expert in the area of computer security. His scholarly activity has been aided by a grant from the National Science Foundation. One result was development of a device that protects computers from penetration by unauthorized individuals. Following normal practice in the UW system, Davida signed over patent rights to the Wisconsin Alumni Research Foundation, and WARF applied for a patent in October 1977.

---

[7] Interview with Science Magazine in October 1978 by then NSA Director Vice Admiral B.R. Inman.

[8] Kahn, David, *The Codebreaker,* The Macmillan Company, 1967, p. 690.

[9] In January 1981, the then Director of NSA, B.R. Inman, even went so far as to write this Committee and complain that the Committee had not forwarded a copy of its investigative report, "The Government's Classification of Private Ideas," *prior* to its issuance. As pointed out by Chairman Brooks in reply to Admiral Inman, Congress does not submit its reports to agencies for pre-review. Furthermore, all the material contained in the report was obtained from open hearings and the public record.

[10] Committee on Government Operations report, dated December 2, 1980, entitled "The Government's Classification of Private Ideas," p. 22.

> On April 21, 1978, Davida, one of his graduate students and WARF received in the mail a "Secrecy Order From the Patent and Trademark Office." The order stated that disclosure of the principles involved in Davida's device "might be detrimental to the national security." Davida and everyone else who knew about the device were ordered to say nothing or risk penalties as great as two years in prison and $10,000 fine. Part of the secrecy order permitted Davida to discuss his invention with agents of the U.S. Government and no one else. The secrecy order did not say why the national security was involved, state how long the order would be in effect, or explain any methods of appeal.
>
> * * * * *
>
> Should the executive branch of government be able to prevent a citizen from speaking or publishing without some involvement by the courts? Should the executive branch of government be able to invoke the claim of "national security" without demonstrating that our national security was genuinely threatened? Should defense or intelligence agencies be able to interfere with or inhibit academic research through the patent process? Is censorship an appropriate function of the Patent and Trademark Office? Who will prevent abuses of the secrecy order concept that could frighten professors and stifle research in areas someone in a defense or intelligence agency opposes? [11]

Clearly, NSA's involvement could have a chilling effect on the vigorous research and development that is on-going in the academic community and our domestic computer industry. This industry has been one of the most viable segments of our economy. Its rapid technological advances have been due in large part to being free to openly exchange ideas without government interference. NSA's inherent tendency to classify everything at its highest level is bound to conflict with this broader goal.

A poignant example of this was the issuance of the Data Encryption Standard by the NBS. The DES specifies a method for encrypting 64-bit blocks of cipher (encrypted text) using a user-specified 56-bit key. It was originally devised by IMB over 10 years ago. Later, with NSA's assistance, it was established as a standard by NBS. Even though NBS certified and issued the encryption standard, NSA's involvement was viewed with suspicion. During considerable public debate, allegations were issued by the academic community and others that NSA's involvement in the DES resulted in a smaller key length than was needed. Ostensibly, NSA wanted a key length large enough to provide communications security, but small enough for NSA to be able to read the messages. A similar controversy has again risen with NSA's announcement that it wants to

[11] The secrecy order was initiated by NSA. After a storm of public protest, the secrecy order was rescinded on June 15, 1978.

use a new data encryption algorithm beginning in January 1988. According to an article in Datamation,[12]

> Since NSA hasn't elaborated on its plans, speculation has risen in some quarters that NSA wants to read everyone's encrypted data communications, mainly because it was unable to break DES and wants to replace it with something easier to decrypt. This same argument was also raised years ago when NSA played a hand in defining DES.

Although NSA is widely respected for its technical expertise, that agency has at times involved itself in activities outside the scope of its foreign intelligence and communications security mission. In effect, it has aimed its intelligence expertise at American citizens. NSA's involvement in these activities and its role under NSDD–145 were aptly described by the American Civil Liberties Union during this Committee's hearings: [13]

> It is not necessary to recite the litany of unlawful and improper NSA activities disclosed in Congressional hearings of the mid-1970's; the whole violation of the privacy rights of hundreds of thousands of Americans in the sweeping "Watch List" program known as Operation Minaret and the acquisition of millions of private cable communications under Operation Shamrock are a well-known part of an historical record of intelligence agency abuses that led to the creation of Congressional oversight committees, the enactment of specific statutory authorities such as the Foreign Intelligence Surveillance Act, and an ongoing effort to instill accountability into the intelligence process.
>
> Although NSA still lacks a legislative charter and is still very much an executive creation whose activities are cloaked in extraordinary secrecy, it is not necessary to impute to NSA any residual lawlessness or "bad faith" motivation to question the wisdom of its designated role in NSDD 145's scheme for a "comprehensive and coordinated approach" toward T&AIS [telecommunications and automated information systems] security throughout the Federal Government and the private sector as well. Assuming the best intentions on NSA's part, it still must be asked:
>
> > Do NSA's priorities within the military intelligence establishment inherently conflict with its role as "focal point" for T&AIS security for all government agencies and the private sector under NSDD 145?
> >
> > Will its policies in its role as National Manager be reflective of its primary military/intelligence mission, or will its advice be measured to lesser security needs?

---

[12] Howe, Charles L., "Into the Night," Datamation, dated June 1, 1986, p. 22.
[13] Hearing record, p. 119.

Will NSA's job-related disposition toward secrecy lead it to perform its duties under NSDD 145 with the same avoidance of public scrutiny that marks its day-to-day performance of its primary reponsibilities?

Is NSA's expertise perhaps too arcane for the actual needs of most non-national security agencies, in the sense that the best security programs might well be developed by those in each agency who are most familiar with that particular agency's systems and responsibilities?

It is clear that NSA cannot reasonably be expected to insure that considerations for open government and personal privacy are carefully balanced against perceived exploitation threats in devising sound T&AIS security policy; given the "national security" mindset that that imbues NSDD 145, it is equally clear that the Directive offers no other source for such input within the Executive Branch.

Under the top secret National Security Council Intelligence Directive Number 6 (NSCID No. 6), which is considered by NSA to be its charter, the NSA has always interpreted its mission to be one of foreign intelligence. However, NSA made a major effort during the early 1970's to obtain a charter for domestic surveillance as well. According to James Bamford, author of the Puzzle Palace,[14] NSA avidly sought and strongly supported the so-called Huston Plan [15] during the Nixon Administration. This plan would have authorized NSA to gather intelligence on (1) U.S. citizens using international facilities, and (2) on individuals and groups.[16] The plan was initially approved by President Nixon, but later rescinded because of objections to the illegal nature of the activities contained in the plan.

Over the last decade, NSA has gone out of its way to avoid involving itself in improper, perhaps illegal, activities that it was criticized for earlier. NSA has done so with the knowledge that public support for its important foreign intelligence mission could quickly dissipate if that agency resorted to abusive practices. NSDD–145 thrusts NSA into the mainstream of the social and economic activities of our country. This is an arena that NSA is uncomfortable with and ill-suited for. That agency's activities under the Directive could lead to the obstruction of the free flow of information to our businesses, schools, and citizens—all in the name of national security.

The inappropriateness of assigning NSA the lead role in a government-wide computer security program under NSDD–145 was, perhaps, best summed up in an editorial in the Baltimore Sun in April of this year.[17]

---

[14] Bamford, James, *The Puzzle Palace:* A Report on America's Most Secret Agency, Penguin Books, 1982

[15] Named after Tom Charles Huston who worked as counsel in the Nixon White House in the late 1960's and early 1970's.

[16] According to James Bamford, NSA had been targeting U.S. citizens throughout the 1960's and early 1970's without authority to do so.

[17] Insecurity by Directive, Baltimore Sun, April 29, 1986

> . . . a new security system must add to, not lessen, the user's confidence in the privacy of their communications. They way to do that is not to submit civilian messages to Pentagon censors, but to develop a system civilians themselves control. The NSA is the wrong agency to handle the job. Too much control is as dangerous as too little.

An example of the dangers that could be involved surfaced late last year when it publicly revealed that NSA was investigating the computer program that counted more than one-third of all the votes cast in the United States.[18] Ostensibly, NSA was performing this investigation under the authorities assigned to it by NSDD–145 in order to determine whether the computer system was vulnerable to fraudulent manipulation. As part of its work on this system, the agency gained detailed knowledge into the functioning of the computer program and any inherent weaknesses within the system that could be tampered with. The central focus of NSA's investigation was the vote-counting program of Computer Election Systems of Berkeley, California, which is apparently the dominant company in the manufacture and sale of computer voting apparatus. According to the New York Times, the company's program and related equipment was used in more than 1,000 county and local jurisdictions to collect and count 34.4 million of the 93.7 million votes cast in the United States.

The Committee does not suggest that what NSA attempted to do was illegal or done with any malice. The question is whether it is proper for a super-secret agency that operates without public scrutiny to involve itself in domestic activities, particularly our country's election process.

CONCLUSION

The Committee believes that H.R. 2889 provides the necessary legislative authority for the government to initiate and implement a strong and viable computer security program which will benefit both Federal agencies and ultimately the private sector. There is no question that such a program is urgently needed. Too much information and data (personal, economic, financial) is being left unprotected in our government's computer and communications systems. Adequate protection must be provided to these systems and H.R. 2889 provides the right measures in terms of training, awareness, research and standards to accomplish this important goal.

H.R. 2889 also provides a statutory base for NBS to take the government-wide lead in developing a useful and viable computer-security program. Clearly, it is the agency that should spearhead the government's computer security initiatives and be the focal point for (1) implementing these initiatives in the civilian agencies, (2) liaison with the private sector, and (3) representing the interests of the U.S. in the international arena. Further, H.R. 2889 recognizes the expertise of NSA in the area and allows that intelligence agency to continue its traditional role of providing computer security for critical defense missions. The bill also provides a statutory

[18] Burnham, David, "U.S. Examines If Computer Used in '84 Election Is Open to Fraud," New York Times, September 24, 1985, p. A–17.

base for NSA to lend its considerable expertise and resources to NBS in the furtherance of its mission.

SECTION-BY-SECTION ANALYSIS

Section 1. Short title

Section 1 titles the Act as the "Computer Security Act of 1986".

Section 2. Findings

Section 2 contains the findings of the Congress that the Federal Government is highly dependent on outmoded information processing systems which are vulnerable to unauthorized access, disclosure and disruption. The government must increase its efforts to make these computer systems more secure.

Section 3. Establishment of Computer Security Management, Research, and Training Program

Section 3 amends the Act of March 3, 1901 (15 U.S.C. 271-278H), by redesignation of Section 18 as Section 20 and adding new Sections 18 and 19.

Subsection 18(a) gives the National Bureau of Standards the sole authority and responsibility for establishing and conducting a computer security management, research and training program for those systems subject to Section 111 of the Federal Property and Administrative Services Act of 1949 (40 U.S.C. 759) or Chapter 35 of Title 44 U.S.C. The primary emphasis of such program shall be the prevention of computer-related fraud and abuse. NBS shall submit to the Secretary of Commerce the standards and guidelines developed pursuant to Section 111.

Subsection 18(b) directs NBS to (1) determine the extent of vulnerabilities of Federal agencies and their contractors computer and communications system; (2) devise procedures and practices to protect information stored, processed or transmitted by Federal agencies; (3) develop computer security standards and guidelines and offer training assistance to agencies and contractors to increase security awareness; (4) make recommendations to GSA on computer security policies and proposed revisions to regulations in accordance with Section 111 of the Federal Property Act; (5) develop and coordinate with GSA, OPM, and NSA joint computer standards, research and training programs; (6) validate the effectiveness of computer security standards through research, inspection and reporting; (7) act as a liaison between government and private sector to further the goals of computer security awareness; and (8) establish an advisory council.

Subsection 19(a) establishes an Advisory Board within NBS consisting of 12 members appointed by the Secretary of Commerce. Four will be from the computer and communications industry. Four will be from outside the Federal Government but not employed by the computer or communications industry. Four will be from the Federal Government with one being from NSA.

Subsection 19(b) describes the duties of the Advisory Board which includes the identification of relevant issues and keeping NBS and the Secretary of Commerce informed of these issues.

Subsection (c) describes the term of office of each member of the Board.

Subsection (d) describes the rate of compensation for Board members and requires a quorum of seven members before any action is taken.

Subsection (e) allows for travel expenses to be paid for non-government employees.

Subsection (f) allows the Board to use personnel from NBS or other agencies to accomplish its mission.

Section 4. Amendment to Brooks Act

Section 4 amends the Federal Property and Administrative Services Act of 1949.

Subsection (f) requires the Secretary of Commerce to provide scientific and technological advisory services to GSA and other agencies concerning ADP and related systems. It also requires the Secretary to establish uniform ADP and related telecommunications standards as well as computer security standards covered by this Act. The subsection also makes such standards to be compulsory and binding unless waived by the Secretary of Commerce. Notice of such waiver must be sent to the appropriate committees of Congress. It also requires the Administrator of GSA to develop computer security and telecommunications policies and revise its IRM regulations as appropriate. The subsection authorizes the acceptance of gifts, property or reimbursement for its work. Finally, it authorizes research into ADP or related systems, including telecommunications.

Section 5. Training by Federal Agencies in Computer and Telecommunications Security

Subsection 5(a) requires mandatory training for Federal agency personnel and their contractors who are involved in the management, use or operation of ADP or other related systems, including telecommunications.

Subsection 5(b) establishes that training shall start 60 days after the issuance of appropriate regulations. The goals of the training will be to enhance computer security awareness and encourage use of improved computer security practices.

Subsection 5(c) requires OPM to issue regulations relating to the procedures and scope of the mandatory training to be provided and how it will be implemented.

Section 6. Additional Federal Agency Responsibilities for Computer and Telecommunications Security

Subsection 6(a) requires each Federal agency to identify its computer and telecommunications system that contains or transmits unclassified sensitive information that if lost or missused could adversely affect the national interest or the conduct of Federal programs.

Subsection 6(b) requires each Federal agency to develop a computer security plan within one year after enactment of this Act. Copies of the plan will be sent to NBS for comment. The Administrator of GSA is authorized to disapprove of the plan.

Section 7. Authorization of Appropriations

Section 7 authorizes for Fiscal Years 1987, 1988, and 1989 appropriations for NBS such sums as may be necessary to carry out the functions of this Act. Federal agencies are similarly authorized for those fiscal years to carry out the training, planning and system identification functions of this Act.

COST ESTIMATE OF THE CONGRESSIONAL BUDGET OFFICE

The cost estimate prepared by the Congressional Budget Office under Sections 308(a) and 403 of the Congressional Budget Act of 1974 is contained in the following letter from its Director:

U.S. CONGRESS,
CONGRESSIONAL BUDGET OFFICE,
Washington, DC, November 14, 1985.

Hon. JACK BROOKS,
Chairman, Committee on Government Operations,
Rayburn House Office Building, Washington, DC.

DEAR MR. CHAIRMAN: The Congressional Budget Office has prepared the attached cost estimate for H.R. 2889, the Computer Security Act of 1985.

If you wish further details on this estimate, we will be pleased to pvovide them.

With best wishes,
Sincerely,

RUDOLPH G. PENNER.

CONGRESSIONAL BUDGET OFFICE, COST ESTIMATE

1. Bill number: H.R. 2889.
2. Bill title: Computer Security Act of 1985.
3. Bill status: As ordered reported by the House Committee on Government Operations, October 29, 1985.
4. Bill purpose: H.R. 2889 would make a number of changes affecting the security of federal computer and telecommunications systems. It would authorize the appropriation of such sums as may be necessary for fiscal years 1987, 1988, and 1989 to carry out the planning, management, research and training programs required by the bill.

H.R. 2889 would give the National Bureau of Standards (NBS) the sole authority and responsibility to establish and conduct a computer security management, research, and training program for those computer and telecommunications systems subject to the Brooks Act. NBS would be required to develop government-wide standards and guidelines, to conduct research, to develop and coordinate training programs, and to validate the effectiveness of computer and telecommunications security standards through inspection and reporting activities. The bill would direct NBS to establish an advisory council composed of representatives of other federal agencies, and to establish within NBS a Computer and Telecommunications Privacy and Security Advisory Board.

Within six months after the date of enactment, H.R. 2889 would require all federal agencies to identify each computer and related

telecommunications system that stores or transmits sensitive data. Within a year after the date of enactment, each agency would be required to establish a plan for the security for each computer and related telecommunications systems previously identified.

Finally, the bill would require mandatory periodic training in computer and telecommunications security for all federal agency employees who manage, use or operate computer or other automated information systems. Similar training would also be required for employees of private contractors who are involved with the management, use or operation of computers that interface with government systems.

5. Estimated cost to the Federal Government: CBO estimates that enactment of this bill would cost NBS about $1 million in 1986 and $4 million to $5 million annually beginning in 1987. Additional costs for planning and training in computer security by all agencies throughout the federal government would probably cost $15 million to $20 million annually beginning in 1987, while planning costs of $5 million to $10 million would likely be incurred in 1986. To the extent that this legislation would reduce fraud or other financial losses, some savings could also result from enactment of H.R. 2889. It is not possible to quantify these potential savings at this time.

Basis of estimate: Under the National Security Decision Directive (NSDD) 145, which became effective in September 1984, the President gave the National Security Agency (NSA) responsibility for ensuring the security of all classified and certain other sensitive information transmitted by federal computers or telecommunications systems. If enacted, H.R. 2889 would assign some of this authority to NBS, mainly in the area of unclassified data. Although under current guidelines it is expected that most federal agencies, with assistance from NSA, would have strengthened security efforts consistent with the directive, this bill would enhance the role of NBS and would also impose new requirements upon federal agencies and their contractors in the area of computer and telecommunications security.

National Bureau of Standards: Assuming enactment of H.R. 2889 by January 1986, the expanded role of NBS in computer security management and training, and its new role in telecommunications policy and security, are estimated to cost up to $1 million in 1986, and about $2 million annually beginning in 1987. Based on information from NBS, an estimated $2 million to $3 million annually may also be needed for research, beginning in 1987. This assumes that NBS would expand its management and oversight role, but would also receive assistance and information from the National Computer Security Center (NSCS) within the Department of Defense (DoD).

Government-wide computer security plans: The level of computer security varies greatly among the approximately 80 federal entities, including about 1,300 different organizations that would be affected by this legislation. The cost of identifying all sensitive computer systems and developing an appropriate plan for facility, application and personnel security would thus vary greatly from agency to agency, depending upon the agency's current level of se-

curity, the size and number of sites, and the resources and expertise available to implement this provision.

In the time available, CBO could not contact each major federal entity to determine the cost of identifying and developing these plans for computer security. Most agencies would probably assign existing personnel and resources to this task in order to meet the one-year deadline imposed by H.R. 2889. If approximately 10,000 plans were developed, each requiring about 1–2 work weeks of effort by agency personnel, and two and one-half work days of review by NBS, NSA, and the General Services Administration (GSA), the cost spread among the various federal agencies would be $10 million to $20 million over the fiscal years 1986 and 1987.

Government-wide training: Currently, training resources in the area of computer security are scattered throughout the federal government. A few civilian agencies, such as the Department of Energy, have developed their own computer security training for both classified and unclassified systems. Most agencies, however, send employees to commercial courses or those offered by other federal agencies, such as GSA, Office of Personnel Management (OPM), the Department of Agriculture Graduate School, or NSA.

H.R. 2889 would require mandatory training for all federal and contractor personnel who manage, use or operate computer or telecommunications systems. The cost of such training depends on the number of people involved and the king of training provided. Based on information from a number of agencies, it expected that roughly half of all government and contractor employees would initially receive some type of training as a result of the bill, or about 3 million employees. Subsequently, training would be provided to most new employees, and retraining would be required only periodically.

It is expected that most training in the area of computer security would become decentralized, with each agency responsible for developing its own programs, although some centralized training for smaller agencies and in specialized program areas would remain. The NCSC is developing a data base of educational opportunities offered by government, universities and private sources, and plans to make this available to agencies. Training courses are relatively expensive, however. They currently cost about $50 to $200 per day per person (not including development costs) and typically are offered to technical personnel who attend a three-to-five day session. In an effort to reduce training costs, NCSC is developing training packages that will be available on tape or film, sharply reducing the training cost per person.

Based on information from NCSC, GSA, OPM, and OMB, CBO made a number of assumptions about the numbers and types of training that would be required as a result of enactment of H.R. 2889. The resulting estimates provide a rough estimate of the possible additional cost of training, but should not be considered precise.

Within three years after the date of enactment, it is assumed that about 90 percent of the estimated 3 million employees affected by the bill would receive some type of computer security awareness training. Assuming the availability of training modules and other low-cost products, it is expected that the cost for this type of training would have no significant budget impact over and above the cost of maintaining good information systems, which is now the re-

sponsibility of each agency. It is estimated that about 10 pecent of the 3 million employees, or 300,000, would require more formalized training. Assuming that about three-quarters of these individuals (about one-half from DoD) would have received training under current law, then about 75,000 employees would likely require training as a result of this bill. Three days of specialized training, at an average cost of $100 per day, for 75,000 persons would cost $20 million to $25 million over several years.

Finally, it is assumed that about 250 civilian employees would gradually be recruited and/or trained to evaluate the technical protection capabilites of industry and government-developed systems, and to train other agency personnel. This type of training, according to NCSC, takes two to three years. At an average cost of $60,000 per year, including overhead, it is estimated that this type of support staff would cost the federal government about $15 million annually, once fully implemented.

6. Estimated cost to State and local governments: State and local governments that have computer or telecommunications systems that interface with those of the federal government would be required to train appropriate staff in computer security. Because no complete inventory of these systems currently exists, it is not possible to estimate the cost at this time.

7. Estimate comparison: None.

8. Previous CBO estimate: None.

9. Estimate prepared by: Mary Maginniss.

10. Estimate approved by: James L. Blum, Assistant Director for Budget Analysis.

Inflationary Impact

In compliance with clause 2(l)(4) of House Rule XI, it is the opinion of the Committee that the provisions of this bill will have no inflationary impact on prices and costs in the operation of the national economy.

Oversight Findings

The Committee has maintained continuous oversight of the government's acquisition and use of information technology. The Committee's findings are incorporated into this report.

New Budget Authority and Tax Expenditures

No new budget authority or tax expenditures are required by the legislation.

Budget Analysis and Projection

The bill provides for new authorization rather than new budget authority. Therefore, the provisions of Section 308(a) of the Congressional Budget Act are not applicable.

Changes in Existing Law Made by the Bill, As Reported

In compliance with clause 3 rule XIII of the Rules of the House of Representatives, changes in existing law made by the bill, as reported, are shown as follows (existing law proposed to be omitted is

enclosed in black brackets, new matter is printed in italic, existing law in which no change is proposed is shown in roman):

ACT OF MARCH 3, 1901

AN ACT To establish the National Bureau of Standards

* * * * * * *

SEC. 18. (a) The National Bureau of Standards shall have the sole authority and responsibility for establishing and conducting a computer security management, research, and training program pertaining to computer and telecommunications systems that are subject to the provisions of section 111 of the Federal Property and Administrative Services Act of 1949 (40 U.S.C. 749) or chapter 35 of title 44, United States Code. The primary emphasis of such program shall be the prevention of computer-related fraud and abuse. For such purpose, the Bureau shall prepare and submit to the Secretary of Commerce, for promulgation under such section 111, government-wide standards and guidelines.

(b) In carrying out the program described in subsection (a), the Bureau shall—

(1) perform research and conduct studies to determine the nature and extent of the vulnerabilities of computer and telecommunications systems in Federal agencies and their contractors;

(2) devise management, administrative, technical, and physical procedures and practices designed to protect the information stored, processed, and transmitted by Government computer and telecommunications systems;

(3) develop standards and guidelines for the security of such computer and telecommunications systems and offer assistance for use by Federal agencies in training their employees, and the employees of their contractors and of other organizations whose computer or telecommunications systems interface with Government computer systems, in computer and telecommunications security awareness and accepted security practices;

(4) make recommendations to the General Services Administration on computer and telecommunications security policy and on revisions of regulations proposed pursuant to section 111(f)(3) of the Federal Property and Administrative Services Act of 1949;

(5) develop and coordinate, as appropriate, with the General Services Administration, the Office of Personnel Management, and the National Security Agency, joint computer and telecommunications security standards, research, and training programs;

(6) validate the effectiveness of computer and telecommunications security standards through research, inspection, and reporting activities;

(7) act as liaison between the Federal Government and the private sector with respect to computer and telecommunications security issues involving sensitive but unclassified information and assist the private sector in using and applying the results of the programs and activities under this section; and

(8) establish an advisory council composed of representatives of other Federal agencies.

SEC. 19. (a) There is hereby established a Computer and Telecommunications Privacy and Security Advisory Board within the National Bureau of Standards. The Secretary of Commerce shall appoint the chairman of the Board. The Board shall be composed of twelve additional members appointed by the Secretary of Commerce as follows:

(1) four members from outside the Federal Government who are eminent in the computer or telecommunications industry, at least one of whom is representative of small or medium sized companies in such industry;

(2) four members from outside the Federal Government who are eminent in the fields of computer or telecommunications technology, or related disciplines, but who are not employed by or representative of a producer of computer or telecommunications equipment; and

(3) four members from the Federal Government who have computer or telecommunications systems management experience, including experience in computer security or telecommunications security, at least one of whom shall be from the National Security Agency.

(b) The duties of the Board shall be—

(1) to identify emerging managerial, technical, administrative, and physical safeguard issues relative to computer and telecommunications systems security; and

(2) to advise the Bureau of Standards and the Secretary of Commerce on security and privacy issues pertaining to computer and telecommunications systems of the Federal Government.

(c) The term of office of each member of the Board shall be four years, except that—

(1) of the initial members, three shall be appointed for terms of one year, three shall be appointed for terms of two years, three shall be appointed for terms of three years, and three shall be appointed for terms of four years; and

(2) any member appointed to fill a vacancy in the Board shall serve for the remainder of the term for which his predecessor was appointed.

(d) The Board shall not act in the absence of a quorum, which shall consist of seven members. Members of the Board, other than full-time employees of the Federal Government, may be compensated at a rate not to exceed the maximum rate of pay for grade GS–18, as provided in subchapter III of chapter 53, title 5, United States Code, when engaged in the actual performance of duties vested in the Board.

(e) Members of the Board, other than full-time employees of the Federal Government, while attending meetings of such committees or while otherwise performing duties at the request of the Board Chairman while away from their homes or a regular place of business, may be allowed travel expenses in accordance with subchapter I of chapter 57 of title 5, United States Code.

(f) To provide the staff services necessary to assist the Board in carrying out its functions, the Board may utilize personnel from the

National Bureau of Standards or any other agency of the Federal Government with the consent of the head of the agency.

SEC. [18.] *20.* Appropriations to carry out the provisions of this Act may remain available for obligation and expenditure for such period or periods as may be specified in the Acts making such appropriations.

SECTION III OF THE FEDERAL PROPERTY AND ADMINISTRATIVE SERVICES ACT OF 1949

AUTOMATIC DATA PROCESSING EQUIPMENT

SEC. 111. (a) * * *

* * * * * * *

[(f) The Secretary of Commerce is authorized (1) to provide agencies, and the Administrator of General Services in the exercise of the authority delegated in this section, with scientific and technological advisory services relating to automatic data processing and related systems, and (2) to make appropriate recommendations to the President relating to the establishment of uniform Federal automatic data processing standards. The Secretary of Commerce is authorized to undertake the necessary research in the sciences and technologies of automatic data processing computer and related systems, as may be required under provisions of this subsection.]

(f)(1) The Secretary of Commerce shall—

(A) provide agencies, and the Administrator in the exercise of functions delegated in this section, with scientific and technological advisory services relating to automatic data processing and related systems, including telecommunications systems;

(B) establish uniform Federal automatic data processing and related telecommunications standards and guidelines; and

(C) on the basis of standards and guidelines developed by the National Bureau of Standards pursuant to section 18(b)(3) of the Act of March 3, 1901 (15 U.S.C. 271 et seq.), establish standards and guidelines for the security of computer and telecommunications systems that are subject to this section.

(2) The standards established by the Secretary of Commerce under paragraphs (1)(B) and (1)(C) shall be compulsory and binding on each Federal agency unless waived by the Secretary of Commerce in writing upon a determination that compliance would adversely affect the accomplishment of the agency's mission or cause a major adverse financial impact on the agency which is not offset by governmentwide savings. Notice of each such waiver shall be promptly transmitted to the Committee on Government Operations of the House of Representatives and the Committee on Governmental Affairs of the Senate.

(3) The Administrator shall ensure that such standards and guidelines are implemented within an integrated information resources management system (as required by chapter 35 of title 44, United States Code) by—

(A) developing and implementing policies on the security of automatic data processing and related telecommunications systems; and

(B) revising the Federal information resources management regulations (41 CFR ch. 201) consistent with such standards, guidelines, and policies.

(4) In carrying out functions under paragraph (1) of this subsection, the Secretary of Commerce and the Director of the National Bureau of Standards are authorized—

(A) to accept, hold, administer, and use gifts and bequests of property, both real and personal, for the purpose of aiding or facilitating such functions; and

(B) to accept reimbursement for the performance of such functions for the benefit of another Federal agency or for the benefit of any other person or organization, at rates approximating the costs thereof.

(5) The Secretary is authorized to undertake the necessary research in the sciences and technologies of automatic data processing computer and related systems, including telecommunications systems, as may be required under the provisions of this subsection.

* * * * * * *

○